Hogan Lovells

Cloud Computing: A Primer on Legal Issues, Including Privacy and Data Security Concerns

Privacy and Information Management Practice / Washington, DC

Disclaimer

- THIS PRESENTATION IS TO ASSIST IN A GENERAL UNDERSTANDING OF THE LEGAL ISSUES SURROUNDING CLOUD COMPUTING. IT IS NOT INTENDED, NOR SHOULD IT BE REGARDED, AS LEGAL ADVICE. COMPANIES OR INDIVIDUALS CONTEMPLATING ENTRY INTO A CLOUD COMPUTING CONTRACT OR HAVING PARTICULAR QUESTIONS SHOULD SEEK THE ADVICE OF COUNSEL.

Overview

- Privacy and Data Security Concerns
- Privacy and Data Security Laws and Regulations
  - Federal Laws
    - Compelled Governmental Disclosure
    - Data Security and Breach Issues
    - Section 5 of the FTC Act
  - State Laws
    - Data Security Issues
    - Data Breach Issues
- Data Breaches/Breach Responsibility
- Information Ownership and Control
- How Cloud Customers Can Manage Risk

Privacy and Data Security Concerns

- Major cloud computing privacy concerns:
  - Compelled disclosure to the government
    - Information stored on the cloud is subject to different protections than information stored in-house
  - Data security and disclosure of breaches
    - Generally, how does a cloud provider protect a customer's data?
    - When the law imposes data security requirements on a customer, how can the customer ensure its compliance when storing information on the cloud?
    - If the cloud's security is breached, must the cloud give notice of the breach?
  - Transfer of, access to, and retention of data
    - Will companies and consumers have access to data on the cloud? Can the cloud confirm the destruction of data or return it?
  - Location of data
    - The physical location of the server storing the data may have legal implications
  - Consumer notice and choice
    - For companies who will store consumers' data on the cloud

Privacy and Data Security Laws and Regulations

- Compelled disclosure to the government
  - Electronic Communications Privacy Act (ECPA); Stored Communications Act (SCA)
  - USA Patriot Act (including National Security Letters; FISA warrants)
  - Warrants and Subpoenas Generally
- Data security issues and data breach notification
  - Family Educational Rights and Privacy Act (FERPA)
  - Gramm-Leach-Bliley Act (GLBA)
  - Health Insurance Portability and Accountability Act (HIPAA)
  - Health Information Technology for Economic and Clinical Health (HITECH) Act
  - Sarbanes Oxley
  - State Laws and Regulations
  - Section 5 of the FTC Act (for companies who will store consumer information on the cloud)

Compelled Disclosure to the Government – ECPA (Including SCA)

- Enacted in 1986
  - No one was thinking of cloud computing
- Protects electronic communications while in transit and while held in storage from disclosure
  - Gives different levels of protection to electronic data based on outdated distinctions like whether it is stored in “electronic storage,” or by a “remote computing service” and how old the data is
  - For example, information stored on a “remote computing service” that is older than 180 days is subject to Gov’t search with just an administrative subpoena
- Problems arise with how to characterize cloud computing activity

Compelled Disclosure to the Government – USA Patriot Act

- Originally enacted in 2001, amended in 2005
- Allows FBI access to certain business records with a court order
- Also provides for use of National Security Letters (form of administrative subpoena) to obtain records
- The law limits the ability of cloud providers to reveal that they received an order
  - Cloud users may not even know about a disclosure

Data Security Issues – Federal Laws, Regulations, and Standards

- Federal laws & regulations:
  - Certain Federal laws and regulations impose industry-specific data security and/or breach notification obligations
    - Financial institutions (GLBA)
    - Educational institutions (FERPA)
    - Health care (HIPAA and HITECH)
    - Publicly traded companies (SOX)
      - Generally, an entity cannot contract away its obligation to comply with these industry-specific regimes
      - Some of these statutes, however, require an entity to pass these obligations to cloud providers by contract
- Federal administrative guidance
  - White House CIO Council, which released data security guidelines for federal agency use of cloud computing and
- Industry standards
  - Payment Card Industry Data Security Standards (PCI DSS) for credit card data

White House CIO Council – Federal Administrative Guidance

- Released as a draft on November 2, 2010
  - Final version to be released after public comments
- Produced by the Federal Risk and Authorization Management Program (FedRAMP)
  - Interagency effort aimed at consolidating risk management activities related to cloud computing
- Proposes standards for cloud computing
  - Common security baseline
  - Continuous monitoring

Data Security Issues – Federal Laws, Regulations, and Standards (continued)

- Some cloud service providers offer “take it or leave it contracts”
- Some cloud providers offer no transparency into their security programs
- Without notice, transparency and communication, it may be impossible for a cloud user to know if it’s complying with data security and breach notification requirements imposed by federal statutes and regulations

Section 5 of the FTC Act (if applicable)—Will the FTC Take Lead on Privacy and Security in the Cloud?

- The FTC has not done a lot in the cloud computing area
- The FTC's December 2010 draft report on privacy highlighted cloud computing as one of the technologies that makes changes to the existing privacy framework necessary
  - But it does not offer prescriptive advice for what sort of notice and choice must be given to consumers by entities who store consumer information on the cloud
- However, entities that store consumer information on the cloud face the threat of FTC enforcement if their representations to consumers about where and how information is stored and secured do not match their actual practices

Data Security Issues – State Laws

- Many states also impose data security requirements on entities operating in the state or who hold data about state residents
  - State data protection laws
  - State data breach laws
- Much like the federal statutes discussed, some state laws obligate entities to receive contractual guarantees that technology vendors will provide adequate information security

State Laws: Massachusetts

- Massachusetts has an extensive data security legal regime
- Regulations provide that businesses must “take reasonable steps to select and retain” third-party service providers
- Regulators have not clarified or explained what this means
  - It potentially could be read to impose an audit or assessment requirement before a business can use a cloud provider

State Laws: Data Breach Notification

- Data breach notification
  - 46 states, DC, Puerto Rico, and the U.S. Virgin Islands have data breach notification statutes for breaches of sensitive information
    - State law varies: 37 states have some risk of harm threshold; each state has its own definition of protected information
  - Usually requires notification of all affected individuals if sensitive information is lost or exposed in a manner that creates a risk of identity theft
  - Notification must be made in a reasonable period of time, though in certain circumstances may be delayed by a government investigation into the breach

Data Breach Responsibility

- Under state data breach laws, the data host (cloud provider) is responsible for breach notification (hacking, lost data, unauthorized access) **to the data owner,** but not to individuals
  - The data owner is ultimately responsible for the breach
  - The parties can agree by contract on who will perform notification duties and functions
- The parties can agree about who will be financially responsible for the breach
  - This might include: notification costs, legal costs (indemnification), investigation costs (such as IT forensic firms), and reputational costs

Information Ownership and Control Issues

- Who owns data on the cloud?
- Can a cloud provider use the data for its own purposes? What if it's de-identified or aggregated?
- When and under what circumstances can the customer obtain a copy of information stored on the cloud?
- When a customer leaves the cloud, what obligations does the provider have to assist in the transition?
- What happens when service to the cloud is interrupted?

How to Deal with Cloud Computing Legal Issues

- Contract! Almost all issues can be dealt with contractually:
  - Where data can be stored
  - What security standards the cloud provider will adhere to
    - Is customer data segregated
    - Does the cloud conform to industry standards
    - Do outside auditors confirm its security practices
  - Who is liable for a data breach
  - Regulatory compliance and indemnification responsibilities
  - Ownership and control of information and availability and maintenance of the cloud
  - See the checklist for more at (hyperlink)

What if I can't negotiate?

- Perform a cost/benefit analysis when choosing a provider
  - What is the reputational risk to the cloud provider if something goes wrong?
    - Consider the company's current reputation for quality, compliance, and best practice
  - What is the reputational risk to your company if something goes wrong?
    - What data will you store on the cloud?
    - How sensitive is this data?

www.hoganlovells.com

Hogan Lovells has offices in:

Abu Dhabi	Caracas	Hong Kong	Munich	Shanghai
Alicante	Colorado Springs	Houston	New York	Silicon Valley
Amsterdam	Denver	Jeddah*	Northern Virginia	Singapore
Baltimore	Dubai	London	Paris	Tokyo
Beijing	Dusseldorf	Los Angeles	Philadelphia	Ulaanbaatar*
Berlin	Frankfurt	Madrid	Prague	Warsaw
Boulder	Hamburg	Miami	Riyadh*	Washington DC
Brussels	Hanoi	Milan	Rome	Zagreb*
Budapest*	Ho Chi Minh City	Moscow	San Francisco	

* Associated offices